UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,200	03/08/2001	Daryl Carvis Cromer	RPS9 2000 0070	6701

7590 05/04/2005

IBM Corporation
Personal and Printing Systems Group
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/802,200	CROMER ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on December 14, 2004 has been entered. Claims 1-53 are pending. Claims 1, 2, 9, 10, 14, 18, 22, 26, 30, 34, 35, and 49 are amended by applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4-14, 16-22, 24-30, 32-38, 40, 42-47, 49-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (US 6,154, 543), and further in view of Chandra et al (US 4,817,140).

a. *Referring to claim 1:*

i. Baltzley teaches:

(1) said system comprises a plurality of client computers and a server **[i.e., the public key cryptosystem with roaming user capability comprises a network having multiple client computers and multiple encryption servers. The network allows secure communication between the client computers and the encryption servers (column 2, lines 21-25)]**,

(2) said server generates a secure transfer key pair and encrypts a private key of said secure transfer key pair **[i.e., as depicted in Figure 3 (see associated descriptions for details)]**,

(3) said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form **[i.e., the Enabler computer program communicates with the Server computer program to enable a user to both read encrypted digital messages sent to him or her and send encrypted digital messages to other users. To read encrypted digital messages sent to a user, the**

user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)], and

(4) each client computer in said plurality thereof is programmed to generate token data including said portion of said token data encrypted with a public key of said secure transfer key pair, to record said token data on a computer readable medium, to read said token data from said computer readable medium, to decrypt said private key of said secure transfer key pair, and to decrypt said portion of said token data with said private key of said secure transfer key pair **[i.e., as depicted in Figures 5 and 7 (see associated descriptions for details in column 5, lines 8-61 and column 6, line 53 through column 7, line 11)]**.

ii. However, Baltzley does not explicitly mention:

(1) encrypted/decrypted portion of token data.

iii. Chandra, on the other hand, teaches:

(1) In accordance with Chandra's invention software can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission). The software is partitioned into an encrypted portion P.sub.e and an unencrypted (clear text) portion P.sub.c. The choice of the partitioning is made by the software vendor with the understanding that only the encrypted portion will be protected from piracy. The encrypted portion, P.sub.e of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems **(column 3, lines 52-66).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention/include a software asset protection mechanism (in Baltzley) which is based on the separation of the software to be protected from the right to execute that software **(see abstract of Chandra).**

v. The ordinary skilled person would have been motivated to:

(1) mention/include a software asset protection mechanism (in Baltzley) because the typical software purchaser may still duplicate at will the software he has received from the vendor. However, he cannot duplicate the right to use the software; in fact he receives a single right to use the software **(column 3, lines 39-43 of Chandra).**

b. *Referring to claim 2:*

i. Baltzley further teaches:

(1) wherein each client computer in said plurality thereof generates a platform key pair, a public key of said platform key pair is transferred to said server **[i.e., as depicted in Figure 5 (see associated descriptions for details)],** and

(2) said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair encrypted with said public key of said platform key pair of said client computer, and each client computer in said plurality thereof stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair **[i.e., as depicted in Figures 5 and 7 (see associated descriptions for details in column 5, lines 8-61 and column 6, line 53 through column 7, line 11)].**

c. *Referring to claim 4:*

i. Baltzley further teaches:

(1) wherein each client computer within said plurality of client computers is enabled to perform a predetermined task in response to decrypting said portion of said token data **[i.e., in order to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then**

hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 40-48)].

d. *Referring to claim 5:*

i. Baltzley further teaches:

(1) each client computer in said plurality of client computers includes an input device for providing a numeric input **[i.e., referring to Figures 1 and 2, a client machine 110 includes a keyboard (not label) for entering input data (see associated descriptions for details),**

(2) said portion of said token data includes a PIN, each client computer in said plurality of client computers, after decrypting said portion of said token data read from said computer readable medium, compares said PIN included within said token data with said numeric input provided through said input device, and each client computer within said plurality of client computers is enabled to perform a predetermined task in response to determining an equivalence between said PIN and said numeric input provided through said input device **[i.e., the Enabler computer program communicates with the Server computer program to enable a user to both read encrypted digital messages sent to him or her and send encrypted digital messages to other users. To read encrypted digital messages sent to a user, the user is first prompted for a passphrase (which includes PIN or password). The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received. In addition, Baltzley's invention provides an important technical advantage by providing a way to securely store a user's private key on an encryption server by symmetrically encrypting it with a passphrase so that no one but the user has access to it (column 2, lines 38-58)].**

e. *Referring to claim 6:*

i. Baltzley further teaches:

(1) said system additionally comprises a communications network connecting said server with each of said client computers in said plurality thereof **[i.e., Figure 1 shows one embodiment of the public key cryptosystem with roaming user capability 200 of the present invention within a communication network system 1000 comprising an encryption server 105 connected to a network of multiple client machines 110 through communication channels 115 which may each be comprised of a secure socket layer. The public cryptosystem with roaming user capability 200 may have a firewall or any other security devices placed between the encryption server 105 and the client machines 110 to further secure the encryption server 105 from being hacked or broken into (column4, lines 6-16)]**, and

(2) said secure transfer key is transmitted over said communications network from said server to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in said encrypted form **[i.e., referring to Figure 6, in step 620, the encryption server 105 authenticates the hashed passphrase and transmits the encrypted private key 320 back to the client computer 110 (column 6, lines 9-12)].**

f. *Referring to claim 7:*

i. Baltzley further teaches:

(1) wherein each client computer in said plurality thereof generates a platform key pair and transmits a public key of said platform key pair to said server over said communications network, said server transmits said secure transfer key pair over said communications network to each of said client computers in said plurality thereof with said platform key pair of said client computer, and each client computer in said plurality thereof stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair **[i.e., the client computer executes a New**

User computer program and an Enabler computer program to facilitate secure communication. Both the New User computer program and the Enabler computer program communicate with a Server computer program located on the encryption server. The New User computer program communicates with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. The private key is then encrypted with the user passphrase yielding an encrypted private key, which is transmitted with the public key to the encryption server. The Enabler computer program communicates with the Server computer program to enable a user to both read encrypted digital messages sent to him or her and send encrypted digital messages to other users. To read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 26-47)].

g. *Referring to claim 8:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

h. *Referring to claim 9:*

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

i. *Referring to claim 10:*

i. Baltzley teaches:

(1) receiving a secure transfer key pair generated within a server; storing said secure transfer key pair **[i.e., referring to Figure 3, the private key is then encrypted with the user passphrase yielding an encrypted private key, which is transmitted with the public key to the encryption server 105 for storing (column 2, lines 35-37). As a matter of fact, once the passphrase is hashed and transmitted to the encryption server for authentication. The New User computer**

program communicates with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. Once the hashed passphrase is authenticated, the encryption server transmits (emphasis added) the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 44-48 and refer to Figure 6 for further details). It is further understood that a client machine or computer or device is also a client/server. The rejection is also applied to those claims with similar limitations];

(2) after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair; and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium **[i.e., the Enabler computer program and the Server computer program also work in conjunction to send encrypted digital messages. Once a digital message is generated, it is encrypted with a client recipient's public key. The encrypted message is then transmitted to the client recipient computer (column 2, lines 49-57)];** and

(3) after storing said secure transfer key pair, in response to an indication that token data is to be read, reading said token data from a computer readable medium, and decrypting a portion of said data with a private key of said secure transfer key pair **[i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 40-48)].**

ii. However, Baltzley does not explicitly mention:

(1) encrypted/decrypted portion of token data.

iii. Chandra, on the other hand, teaches:

(1) In accordance with Chandra's invention software can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission). The software is partitioned into an encrypted portion P.sub.e and an unencrypted (clear text) portion P.sub.c. The choice of the partitioning is made by the software vendor with the understanding that only the encrypted portion will be protected from piracy. The encrypted portion, P.sub.e of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems **(column 3, lines 52-66).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention/include a software asset protection mechanism (in Baltzley) which is based on the separation of the software to be protected from the right to execute that software **(see abstract of Chandra).**

v. The ordinary skilled person would have been motivated to:

(1) mention/include a software asset protection mechanism (in Baltzley) because the typical software purchaser may still duplicate at will the software he has received from the vendor. However, he cannot duplicate the right to use the software; in fact he receives a single right to use the software **(column 3, lines 39-43 of Chandra).**

m. *Referring to claims 11, 19, 27, 35, 47, and 52:*

i. These claims have limitations that is similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

k. *Referring to claims 12, 20, 28, 36, and 40:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

l. *Referring to claim 13:*

i. Baltzley further teaches:

(1) wherein said secure transfer key pair is read from

a computer readable medium **[i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 40-48)]**.

m. *Referring to claims 14, 22, 30, and 38:*

i. These claims have limitations that is similar to those of claims 2 and 7, thus they are rejected with the same rationale applied against claims 2 and 7 above.

n. *Referring to claims 16, 24, 32, and 42:*

i. These claims have limitations that is similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

o. *Referring to claims 17, 25, 33, 43, and 49:*

i. These claims have limitations that is similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

p. *Referring to claims 18 and 26:*

i. These claims have limitations that is similar to those of claim 10, thus they are rejected with the same rationale applied against claim 10 above.

q. *Referring to claims 21, 29, 37, and 53:*

i. These claims have limitations that is similar to those of claim 13, thus they are rejected with the same rationale applied against claim 13 above.

r. *Referring to claim 34:*

i. Baltzley teaches:

(1) generating a secure transfer key pair within a server **[i.e., as a matter of fact, once the passphrase is hashed and transmitted to the encryption server for authentication. The New User computer program communicates with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. Once the hashed passphrase is**

authenticated, the encryption server transmits (emphasis added) the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 44-48 and refer to Figure 6 for further details). It is further understood that a client machine or computer or device is also a client/server. The rejection is also applied to those claims with similar limitations]; transferring a secure transfer key pair from said server to said local computer; storing said secure transfer key pair within said local computer **[i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)];**

(2) establishing communication between said remote computer and said server **[i.e., Baltzley's invention provides another important technical advantage by providing a way to securely store a user's private key on an encryption server so a user may access the private key from any client machine on the encryption server network, thus providing roaming capability (column 2, lines 59-63)];**

(3) transferring said secure transfer key pair from said server to said remote computer; storing said secure transfer key pair within said remote computer **[i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)];**

(4) encrypting said portion of said token data within said local computer with a public key of said secure transfer key pair **[i.e., once a digital**

message is generated, it is encrypted with a client recipient's public key (column 2, lines 51-52)];

(5) recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said local computer on a computer readable medium; transporting said computer readable medium from said local computer to said remote computer; reading said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said remote computer from a computer readable medium; decrypting said portion of said token data within said remote computer with a private key of said secure transfer key pair; and enabling said performance of said predetermined task in said remote computer in response to said portion of said token data **[i.e., as depicted in Figures 5 and 7 (see associated descriptions for details in column 5, lines 8-61 and column 6, line 53 through column 7, line 11; and column 2, lines 38-48)]**.

ii. However, Baltzley does not explicitly mention:

(1) encrypted/decrypted portion of token data.

iii. Chandra, on the other hand, teaches:

(1) In accordance with Chandra's invention software can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission). The software is partitioned into an encrypted portion P.sub.e and an unencrypted (clear text) portion P.sub.c. The choice of the partitioning is made by the software vendor with the understanding that only the encrypted portion will be protected from piracy. The encrypted portion, P.sub.e of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems **(column 3, lines 52-66).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention/include a software asset protection mechanism (in Baltzley) which is based on the separation of the software to be protected from the right to execute that software **(see abstract of Chandra).**

v. The ordinary skilled person would have been motivated to:

(1) mention/include a software asset protection mechanism (in Baltzley) because the typical software purchaser may still duplicate at will the software he has received from the vendor. However, he cannot duplicate the right to use the software; in fact he receives a single right to use the software **(column 3, lines 39-43 of Chandra).**

s. *Referring to claim 44:*

i. This claim has limitations that is similar to those of claim 34, thus it is rejected with the same rationale applied against claim 34 above.

t. *Referring to claim 50:*

i. This claim has limitations that is similar to those of claims 1 and 34, thus it is rejected with the same rationale applied against claims 1 and 34 above.

u. *Referring to claim 51:*

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3, 15, 23, 31, 39, 41, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (US 6,154, 543), and further in view of Taaffe (US 4,747,139).

a. *Referring to claim 3:*

i. Baltzley further teaches:

(1) each client computer in said plurality thereof includes a security subsystem having a subsystem processor and subsystem storage **[i.e., Figure 2 shows a client machine 110 which can comprise incoming and outgoing communication channels 115, a memory 205, and one or more processors 210, such as microprocessors or digital signal processors. Memory 205 can include any storage medium, including RAM, a hard drive, and tape memory. The processors 210 are electrically connected to the memory 205 and have access to a New User computer program 215 and an Enabler computer program 220 (column 4, lines 18-25),**

(2) each client computer in said plurality thereof generates a hardware key pair within said security subsystem, a private key of said platform key pair is encrypted with said hardware public key and is decrypted with said hardware private key in said security subsystem before said private key of said platform key pair is used to decrypt said private key of said secure transfer key pair within said security subsystem **[i.e., the client computer executes a New User computer program and an Enabler computer program to facilitate secure communication. Both the New User computer program and the Enabler computer program communicate with a Server computer program located on the encryption server. The New User computer program communicates with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. The private key is then encrypted with the user passphrase yielding an encrypted private key, which is transmitted with the public key to the encryption server. The Enabler computer program communicates with the Server computer program to enable a user to both read encrypted digital messages sent to him or her and send encrypted digital messages to other users. To read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client**

computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 26-48)].

ii. However, Baltzley does not explicitly mention:

(1) generates a hardware key pair, a private key of said hardware key pair is stored in said subsystem storage.

iii. Whereas, Taaffe teaches:

(1) In one application of the invention, a hardware key generator may be permanently fixed in a computer system and the system may further include means for both encripting and decripting software or data. Prior to transmitting information from the system, as to a storage unit, the information is encrypted using the system encryptor and a key generated by the key generator. The encrypted information is not usable without the key generator module in the system. Preferably the encryptor is positioned between the CPU bus and each input/output controller. Preferably, the key generator provides the encryptor with the key pair for encryption and transmission **(column 3, lines 42-60).** The hardware module may be combined with a storage medium in a software package. The decryption routines and a key sequence to be applied to the key generator are stored with the application software on the storage medium **(see abstract).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) thoroughly point out or include such hardware key generator for generating/storing a hardware key pair (in Baltzley) to protect software from unauthorized copying and unauthorized access **(column 1, lines 13-14 of Taaffe).**

iv. The ordinary skilled person would have been motivated to:

(1) thoroughly point out or include such hardware key generator for generating/storing a hardware key pair (in Baltzley), since unauthorized access to data is a large problem for the data processing community and the military. Unauthorized access can take many forms, from the casual looking at data on a terminal connected to the computer to the theft of some sort of storage medium, disk,

tape, floppy, etc., with subsequent use of the data on another computer **(column 1, line 66 through column 2, line 4 of Taaffe).**

b. *Referring to claims 15, 23, 31, 39, 41, and 48:*

i. These claims have limitations that is similar to those of claims 3 and 7, thus they are rejected with the same rationale applied against claims 3 and 7 above.

Response to Arguments

4. Applicant's arguments filed December 14, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"Baltzley does not disclose, teach, or otherwise anticipate the requirement of claim 1 for the server to generate a secure transfer key pair and to encrypt a private key of the secure transfer key pair.

Examiner totally disagrees with applicant's remarks and maintains that:

Baltzley does teach the claimed subject matter. As a matter of fact, once the passphrase is hashed and transmitted to the encryption server for authentication. The New User computer program communicates with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. Once the hashed passphrase is authenticated, the encryption server transmits (emphasis added) the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 44-48 and refer to Figure 6 for further details). The rejection is also applied to those claims with similar limitations.

Applicant further argues that:

"Baltzley does not anticipate the requirement for each client computer to be programmed to generate token data including the portion of the token data encrypted with a public key of the secure transfer key pair. And that Chandra does not include any teachings that make up for the deficiencies of Baltzley in describing the limitations of claim 1."

Examiner again disagrees and maintains that:

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, as depicted in Figures 5 and 7 of Baltzley (see associated descriptions for details in column 5, lines 8-61 and column 6, line 53 through column 7, line 11 of Baltzley). In accordance with Chandra's invention software can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission). The software is partitioned into an encrypted portion P.sub.e and an unencrypted (clear text) portion P.sub.c. The choice of the partitioning is made by the software vendor with the understanding that only the encrypted portion will be protected from piracy. The encrypted portion, P.sub.e of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems (column 3, lines 52-66 of Chandra). Thus, the combination of teaching between Baltzley and Chandra are well define and efficient to support the previous rejection and repeated herein. The rejection is also applied to those claims with similar limitations.

Applicant further argues that:

"Taaffe does not describe a system exchanging key pairs with a server, including the disclosure of Taaffe to that of Baltzley in describing the limitations of claims 1 and 2, upon which claim 3 depends."

Examiner again disagrees and maintains that:

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teaching between Baltzley/Taaffe are well define and efficient to support the previous rejection and repeated herein. The rejection is also applied to those claims with similar limitations.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. Kaliski, Jr. (US 6,189,098 B1) discloses A protocol for establishing the authenticity of a client to a server in an electronic transaction by encrypting a certificate with a key known only to the client and the server (see abstract).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
April 30, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100